COMPLEX HADAMARD MATRICES OF ORDER 6: A FOUR-PARAMETER FAMILY

FERENC SZÖLLŐSI

Dedicated to Professor Uffe Haagerup on the occasion of his 60th birthday

ABSTRACT. In this paper we construct a new, previously unknown four-parameter family of complex Hadamard matrices of order 6, the entries of which are described by algebraic functions of roots of various sextic polynomials. We conjecture that the new, generic family $G_6^{(4)}$ together with Karlsson's degenerate family $K_6^{(3)}$ and Tao's spectral matrix $S_6^{(0)}$ form an exhaustive list of complex Hadamard matrices of order 6. Such a complete characterization might finally lead to the solution of the famous MUB-6 problem.

1. INTRODUCTION

Complex Hadamard matrices form an important family of orthogonal arrays with the additional unimodularity constraint imposed on their entries. These matrices obey the algebraic identity $HH^* = nI_n$ where $*$ stands for the Hermitean transpose, and I_n is the identity matrix of order n. They appear in various branches of mathematics frequently, including linear algebra [6], coding- and operator theory [7, 15] and harmonic analysis [13, 19]. They play an important rôle in quantum optics, high-energy physics, and they are one of the key ingredients to quantum teleportation- and dense coding schemes [20] and mutually unbiased bases (MUBs) [2]. An example of complex Hadamard matrices is the Fourier matrix F_n, well-known to exists for all n. It is natural to ask how does a "typical" complex Hadamard matrix of order n look like, and a satisfying answer to this question can be given provided we have a complete characterization of Hadamard matrices of order n at our disposal. These types of problems, however, are notoriously difficult even for small n. Naturally, one is interested in the essentially different matrices only, and we identify two matrices H and K and say that they are equivalent if $H = P_1 D_1 K D_2 P_2$ for some unitary diagonal matrices D_1, D_2 and permutational matrices P_1, P_2. Recall that a complex Hadamard matrix is dephased, if all entries in its first row and column are equal to 1. While studying and classifying real Hadamard matrices is naturally a discrete, finite problem which can be handled by deep algebraic methods and sophisticated computer programs to some extent, the complex case, however, behaves essentially different. In particular, due to the appearance of various parametric families one cannot hope for a finite list of inequivalent matrices, but rather for a finite list of constructions, each of them leading to an infinite family of complex Hadamard matrices.

The complete classification of complex Hadamard matrices is available up to order $n = 5$ only. It is trivial that F_n is the unique complex Hadamard matrix for orders $n \leq 3$. The case

$n = 4$ is still elementary, and it was shown by Craigen that all complex Hadamard matrices of order 4 belong to an infinite, continuous one-parameter family [4]. In order 5 we have uniqueness again, a result which is absolutely non-trivial already. In particular, Lovász was the first who showed [12] that F_5 is the only circulant complex Hadamard matrix in this order, and a decade later Haagerup managed to prove the uniqueness of F_5 by discovering an algebraic identity (cf. formula (17)) relating the matrix entries in a surprising way [7].

In order 6 various one- [1, 5, 14, 21], two- [11, 17] and three-parameter families [9, 10] have been constructed recently and it is conjectured that these are part of a more general, four-parameter family of complex Hadamard matrices, yet to be discovered [2]. This conjecture is supported by overwhelming numerical evidence [16], however so far only a fairly small subset of it was described by closed analytic formulæ, including an isolated matrix $S_6^{(0)}$ and a three-parameter matrix $K_6^{(3)}$ [9, 10].

The reason why the 6×6 case received significant attention in the past couple of years is the fact that complex Hadamard matrices are closely related to mutually unbiased bases. Recall that two orthonormal bases of $\mathbb{C}^d$, $\mathcal{B}_1$ and $\mathcal{B}_2$ are unbiased if for every $e \in \mathcal{B}_1$, $f \in \mathcal{B}_2$ we have $|\langle e, f \rangle|^2 = 1/d$. A family of orthonormal bases is said to be mutually unbiased if every two of them are unbiased. The famous MUB-6 problem asks for the maximal number of mutually unbiased bases in $\mathbb{C}^6$. On the one hand this number is at least 3, as there exists various infinite families of triplets of MUBs in this order [8, 17, 21], on the other hand it is well-known that it cannot be larger than 7 (cf. the references of [2]). In fact, it is conjectured that a triplet is the best one can come up with in dimension 6 [21]. The connection between MUBs and Hadamard matrices of order 6 has been exploited in [8] very recently, where a discretization scheme was offered to attack the problem and it was proved by means of computers, however, in a mathematically rigorous way, that the members of the two-parameter Fourier family $F_6^{(2)}(a, b)$ and its transpose cannot belong to a configuration of 7 MUBs containing the standard basis in dimension 6. One reasonable hope to finally settle the MUB-6 problem is to give a complete characterization of complex Hadamard matrices of order 6 and apply the same technique to them.

The goal of this paper is to propose a general framework towards the complete classification of complex Hadamard matrices of order 6. In particular, by characterizing the orthogonal triplets of rows in complex Hadamard matrices we generalize an observation of Haagerup [7] to obtain a new algebraic identity relating the matrix entries in an unexpected way. This is an essentially new tool to study complex Hadamard matrices of small orders, and one of the main achievements of this paper. We apply this result to obtain complex Hadamard matrices, moreover we conjecture that the the construction we present here reflects the true nature of complex Hadamard matrices of order 6. It has the following three features: Firstly, it is general in contrast with the earlier attempts where always some additional extra structure was imposed on the matrices including self-adjointness [1], symmetry [14], circulant block structure [17] or H_2-reducibility [9]. Secondly, it has 4 degrees of freedom and thirdly all the entries of the obtained matrices can be described by algebraic functions of roots of various sextic polynomials. This suggests on the one hand the existence of a four-parameter family of complex Hadamard matrices of order 6 and reminds us on the other hand the fact that the desired algebraical description where the entries are expressed by radicals might not be possible at all. However, from the applicational point of view, and in particular, to utilize the computer-aided attack of [8] to the MUB-6 problem we shall need these matrices numerically anyway.

The outline of the paper is as follows. In Section 2 we briefly discuss the main ideas of the construction to motivate the various auxiliary results we prove there. The excited reader might want to skip this section at first, and jump right ahead to Section 3, where the construction of the new family is presented from a high-level perspective. In Section 4 we analyze the construction thoroughly.

2. Preliminary results

In this section we present the ingredients necessary to construct our new family of complex Hadamard matrices of order 6, including a characterization of the mutual orthogonality of three rows in Hadamard matrices (cf. Theorem 2.4). First, however, we would like to motivate these efforts by describing the main ideas of the construction.

We start with a submatrix

$$(1) \qquad E(a,b,c,d) := \begin{bmatrix} 1 & 1 & 1 \\ 1 & a & b \\ 1 & c & d \end{bmatrix}$$

and attempt to embed it into a complex Hadamard matrix of order 6

$$(2) \qquad G_6^{(4)}(a,b,c,d) := \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & b & e & s_1 & s_2 \\ 1 & c & d & f & s_3 & s_4 \\ \hline 1 & g & h & * & * & * \\ 1 & t_1 & t_3 & * & * & * \\ 1 & t_2 & t_4 & * & * & * \end{array} \right] \equiv \begin{bmatrix} E & B \\ C & D \end{bmatrix}.$$

with 3×3 blocks E, B, C and D in two steps, as follows. First we construct the submatrices B and C featuring unimodular entries to obtain three orthogonal rows and columns of G_6. Secondly we find the unique lower right submatrix D to get a unitary matrix. Should the entries of this matrix become unimodular, we have found a complex Hadamard matrix. We conjecture that the submatrix E can be chosen, up to equivalence, in a way that there will be only finitely many candidates for the blocks B and C and therefore we can ultimately decide whether the submatrix E can be embedded into a complex Hadamard matrix. The resulting matrix G_6 can be thought as the "Hadamard dilation" of the operator E.

We shall heavily use the following through the paper without any further comment: the conjugate of a complex number of modulus 1 is its reciprocal, and hence the conjugate of a multivariate polynomial with real coefficients depending on indeterminates of modulus 1 is just the polynomial formed by entrywise reciprocal of the aforementioned indeterminates. We computed various Gröbner bases [3] in this paper with the aid of Mathematica. The reader is advised to use a computer algebra system for bookkeeping purposes and consult [18] for the standard notations for well-known complex Hadamard matrices such as $S_6^{(0)}, K_6^{(3)}$, etc.

We begin with recalling two elementary results from the existing literature.

Lemma 2.1. *Suppose that we have a partial row* $(1, a, b, e, *, *)$ *composed from unimodular entries. Then one can specify some unimodular numbers* s_1 *and* s_2 *in place of the unknown numbers* $*$ *to make this row orthogonal to* $(1, 1, 1, 1, 1, 1)$ *if and only if*

$$(3) \qquad |1 + a + b + e| \leq 2.$$

Proof. To ensure orthogonality, we need to have $1 + a + b + e + s_1 + s_2 = 0$ from which it follows that $|1 + a + b + e| = |s_1 + s_2| \leq 2$. It is easily seen geometrically, that in this case we can define the unimodular numbers required. □

The missing coordinates featuring in Lemma 2.1, s_1 and s_2, can be obtained algebraically through the well-known

Lemma 2.2 ((Decomposition formula, [14])). *Suppose that the rows* $(1, 1, 1, 1, 1, 1)$ *and* $(1, a, b, e, s_1, s_2)$ *containing unimodular entries are orthogonal. Let us denote by* $\Sigma := 1 + a + b + e$, *and suppose that* $0 < |\Sigma| \leq 2$. *Then*

$$(4) \qquad s_{1,2} = -\frac{\Sigma}{2} \pm \mathbf{i}\frac{\Sigma}{|\Sigma|}\sqrt{1 - \frac{|\Sigma|^2}{4}}.$$

If $\Sigma = 0$ *then* s_1 *is independent from* a, b, e *but* $s_2 = -s_1$.

Proof. Clearly s_1 and s_2 are the unimodular numbers with $s_1 + s_2 = -\Sigma$. □

Now we proceed by investigating the orthogonality of triplets of rows. In order to do this, the following is a crucial

Definition 2.3 ((Haagerup polynomial)). *The Haagerup polynomial* $\mathcal{H}$ *associated to the rows* $(1, 1, 1, 1, 1, 1), (1, a, b, e, *, *)$ *and* $(1, c, d, f, *, *)$ *of a complex Hadamard matrix read*

$$\mathcal{H}(a, b, c, d, e, f) := (1 + a + b + e)(1 + \overline{c} + \overline{d} + \overline{f})(1 + c\overline{a} + d\overline{b} + f\overline{e}).$$

The first result of ours is the following

Theorem 2.4. *Suppose that we have the partial rows* $(1, a, b, e, *, *)$ *and* $(1, c, d, f, *, *)$, *composed from unimodular entries. Then one can specify some unimodular numbers* s_1, s_2, s_3 *and* s_4 *in place of the unknown numbers* $*$ *to make these rows together with* $(1, 1, 1, 1, 1, 1)$ *mutually orthogonal if and only if*

$$(5) \qquad \mathcal{H}(a, b, c, d, e, f) = 4 - |1 + a + b + e|^2 - |1 + c + d + f|^2 - |1 + c\overline{a} + d\overline{b} + f\overline{e}|^2$$

with

$$(6) \qquad |\mathcal{H}(a, b, c, d, e, f)| \leq 8.$$

Proof. First we start by proving that (5) holds. To do this, we utilize Haagerup's idea [7] as follows: by pairwise orthogonality, we find that

$$1 + a + b + e = -s_1 - s_2$$
$$1 + \overline{c} + \overline{d} + \overline{f} = -\overline{s}_3 - \overline{s}_4$$
$$1 + c\overline{a} + d\overline{b} + f\overline{e} = -s_3\overline{s}_1 - s_4\overline{s}_2$$

Now, by multiplying these three equations together we find that (6) follows and further

$$\mathcal{H} = -(s_1 + s_2)(\overline{s}_3 + \overline{s}_4)(s_3\overline{s}_1 + s_4\overline{s}_2) = -(s_1\overline{s}_3 + s_2\overline{s}_4 + s_1\overline{s}_4 + s_2\overline{s}_3)(s_3\overline{s}_1 + s_4\overline{s}_2) =$$

$$-|s_1\overline{s}_3 + s_2\overline{s}_4|^2 - (s_1\overline{s}_4 + s_2\overline{s}_3)(s_3\overline{s}_1 + s_4\overline{s}_2) = -|s_1\overline{s}_3 + s_2\overline{s}_4|^2 - 2\Re(s_1\overline{s}_2 + s_3\overline{s}_4).$$

To conclude the proof, we need to show that

$$2\Re(s_1\overline{s}_2 + s_3\overline{s}_4) = |1 + a + b + e|^2 + |1 + c + d + f|^2 - 4$$

holds, however this follows from the Decomposition formula easily.

To see the converse direction, we need to show that (5) essentially encodes orthogonality. Let us use the notations $\Sigma := 1 + a + b + e$, $\Delta := 1 + c + d + f$, $\Psi := 1 + c\bar{a} + d\bar{b} + f\bar{e}$. With this notation condition (5) boils down to

$$(7) \qquad \mathcal{H} = \Sigma \overline{\Delta} \Psi = 4 - |\Sigma|^2 - |\Delta|^2 - |\Psi|^2.$$

Clearly, if $|\Sigma| \leq 2$ and $|\Delta| \leq 2$ hold, then by the decomposition formula we can find $s_1, s_2,$ s_3 and s_4 to ensure orthogonality to row $(1, 1, 1, 1, 1, 1)$. Now observe, that the mutual orthogonality of rows $(1, a, b, e, s_1, s_2)$ and $(1, c, d, f, s_3, s_4)$ reads

$$(8) \qquad \Psi + s_3 \bar{s}_1 + s_4 \bar{s}_2 = 0.$$

Suppose first that we have the trivial case $\Sigma = \Delta = 0$. Then, by the decomposition formula we have $s_2 = -s_1$ and $s_4 = -s_3$, and (7) implies that $|\Psi| = 2$. Therefore, if we set the unimodular number $s_3 := -\Psi s_1/2$ the orthogonality equation (8) is fulfilled.

Suppose secondly, that we have $\Delta = 0$, but $\Sigma \neq 0$. Then we have $s_4 = -s_3$, and from (7) it follows that $|\Sigma| \leq 2$, and in particular

$$(9) \qquad |\Psi| = \sqrt{4 - |\Sigma|^2}.$$

Now we can use the Decomposition formula to find out the values of s_1 and s_2 and the orthogonality equation (8) becomes

$$(10) \qquad \Psi + s_3 \left(-2\mathbf{i} \frac{\overline{\Sigma}}{|\Sigma|} \sqrt{1 - \frac{|\Sigma|^2}{4}} \right) = 0.$$

This holds, independently of s_3, if $|\Sigma| = 2$, as by (9) $\Psi = 0$ follows. Otherwise, set the unimodular number

$$s_3 := -\mathbf{i} \frac{\Sigma \Psi}{|\Sigma||\Psi|}$$

to ensure the orthogonality through (10).

Finally, let us suppose that $\Sigma \neq 0$ and $\Delta \neq 0$. Now observe that in this case the value of Ψ needed for formula (8) can be calculated through (7). The other ingredient, namely the value of $s_3 \bar{s}_1 + s_4 \bar{s}_2$ can be established through the Decomposition formula, once we derive the required bounds $|\Sigma| \leq 2$ and $|\Delta| \leq 2$. Depending on the value of $\mathcal{H}$, we treat several cases differently.

CASE 1: Suppose that $-|\Psi|^2 \leq \mathcal{H}$. This implies, by formula (7), that $|\Sigma|^2 + |\Delta|^2 \leq 4$, and in particular $|\Sigma| \leq 2$, $|\Delta| \leq 2$ hold. Next we calculate $|\Psi|$ from (7).

Suppose first that $\mathcal{H} \geq 0$. Hence, after taking absolute values, (7) becomes

$$|\Psi|^2 + |\Sigma||\Delta||\Psi| + |\Sigma|^2 + |\Delta|^2 - 4 = 0,$$

and the only non-negative root is

$$(11) \qquad |\Psi| = \frac{-|\Sigma||\Delta| + \sqrt{(4 - |\Sigma|^2)(4 - |\Delta|^2)}}{2}.$$

Now suppose that $-|\Psi|^2 \leq \mathcal{H} < 0$. Hence, after taking absolute values, (7) becomes

$$(12) \qquad |\Psi|^2 - |\Sigma||\Delta||\Psi| + |\Sigma|^2 + |\Delta|^2 - 4 = 0,$$

and we find that the only non-negative root we have under the assumption $|\Sigma|^2 + |\Delta|^2 \leq 4$ reads

$$(13) \qquad |\Psi| = \frac{|\Sigma||\Delta| + \sqrt{(4 - |\Sigma|^2)(4 - |\Delta|^2)}}{2}.$$

CASE 2: Suppose now that $\mathcal{H} < -|\Psi|^2$. This implies that $|\Sigma|^2 + |\Delta|^2 > 4$, and we do not have a priori the bounds $|\Sigma| \leq 2$, $|\Delta| \leq 2$. Nevertheless, we derive equation (12) again, and we find that the values of $|\Psi|$ can be any of

$$(14) \qquad |\Psi|_{1,2} = \frac{|\Sigma||\Delta| \pm \sqrt{(4 - |\Sigma|^2)(4 - |\Delta|^2)}}{2},$$

provided that the roots are real, namely we have either $|\Sigma| > 2$ and $|\Delta| > 2$ or $|\Sigma| \leq 2$ and $|\Delta| \leq 2$. The first case is, however, not possible, as it would imply $|\Psi| > 2$ contradicting the crucial condition (6).

Once we have established the bounds $|\Sigma| \leq 2$, $|\Delta| \leq 2$ and the value(s) of $|\Psi|$ has been found, we are free to use the Decomposition formula to obtain the values of s_1, s_2, s_3 and s_4. Clearly, we can set s_1 with the $+$ sign, while s_2 with the $-$ sign as in formula (4), up to equivalence. However, we do not know a priori how to distribute the signs amongst s_3 and s_4, and to simplify the notations we define

$$(15) \qquad s_3 = -\frac{\Delta}{2} \pm \mathbf{i}\frac{\Delta}{|\Delta|}\sqrt{1 - \frac{|\Delta|^2}{4}}, \quad s_4 = -\frac{\Delta}{2} \mp \mathbf{i}\frac{\Delta}{|\Delta|}\sqrt{1 - \frac{|\Delta|^2}{4}}.$$

In particular, by using (7) and (15) we find that the orthogonality equation (8) becomes

$$(16) \qquad \frac{4 - |\Sigma|^2 - |\Delta|^2 - |\Psi|^2}{\Sigma\overline{\Delta}} + \frac{\overline{\Sigma}\Delta}{2} \pm 2\frac{\overline{\Sigma}\Delta}{|\Sigma||\Delta|}\sqrt{1 - \frac{|\Sigma|^2}{4}}\sqrt{1 - \frac{|\Delta|^2}{4}} = 0,$$

where the $\pm$ sign agrees with the definition of s_3. To conclude the theorem plug in all of the possible values of $|\Psi|$ as described in (11), (13), (14) into (16) to verify that for some choice of the sign it holds identically. $\qquad \square$

Remark 2.5. The two possible signs described by formula (14) can be realized. In particular, there are two different orthogonal triplet of rows composed of sixth roots of unity where $|\Sigma| = |\Delta| = \sqrt{3}$ in both cases, however, in one of the cases $|\Psi| = 1$ while $|\Psi| = 2$ in the other.

Corollary 2.6 ((Haagerup's trick, [7])). *Suppose that the rows $(1, 1, 1, 1, 1, 1)$, $(1, a, b, e, s_1, s_2)$ and $(1, c, d, f, s_3, s_4)$ composed of unimodular entries are mutually orthogonal. Then*

$$(17) \qquad \mathcal{H}(a, b, c, d, e, f) \in \mathbb{R}.$$

Haagerup used the property (17) to give a complete characterization of complex Hadamard matrices of order 5, or equivalently, describe the orthogonal maximal abelian ∗-subalgebras of the 5×5 matrices [7]. Since then it was used in [1] and [14] to construct new, previously unknown complex Hadamard matrices of order 6 as well. However, to guarantee the mutual orthogonality of three rows the necessary condition (17) should be replaced by the more stronger identity (5). Nevertheless, (17) will play an essential rôle in this paper too. These type of identities are extremely useful as they feature less variables than the standard orthogonality equations considerably simplifying the calculations required.

Solving the system of equations (5)–(17) is the key step to obtain the submatrices B and C of G_6. Once we have three orthogonal rows and columns we readily fill out the remaining lower right submatrix D. This is explained by the following two lemmata, the first of which being a special case of a more general matrix inversion

Lemma 2.7. *If U and V are $n \times n$ matrices then*

$$(I_n + UV)^{-1} = I_n - U(I_n + VU)^{-1}V$$

provided that one of the matrices $I_n + UV$ or $I_n + VU$ is nonsingular.

Proof. By symmetry, we can suppose that the matrix $I_n + VU$ is nonsingular. Then, we have

$$(I_n + UV)(I_n - U(I_n + VU)^{-1}V) = I_n + UV - U(I_n + VU)(I_n + VU)^{-1}V = I_n.$$

$\square$

Lemma 2.8. *Suppose that we have a 6×6 partial complex Hadamard matrix consisting of three orthogonal rows and columns, containing no vanishing 3×3 minor. Then there is a unique way to construct a unitary matrix containing these rows and columns as a submatrix.*

Proof. Let U be a 6×6 matrix with 3×3 blocks A, B, C and D, as the following:

$$U = \begin{bmatrix} A & B \\ C & D \end{bmatrix}.$$

By the orthogonality of the first three rows and columns and using the fact that the entries are unimodular, we have

$$(18) \qquad AA^* + BB^* = 6I_3$$

$$(19) \qquad A^*A + C^*C = 6I_3$$

To ensure orthogonality in-between the first three and the last three rows we need to have $AC^* + BD^* = O_3$, the all 0 matrix. As B is nonsingular by our assumptions we can define

$$(20) \qquad D := -CA^*(B^{-1})^*.$$

Now we need to show that the last three rows are mutually orthogonal as well. Indeed, by using (20) and (18) we have

$$CC^* + DD^* = C\left(I_3 + A^*(BB^*)^{-1}A\right)C^* = C\left(I_3 + A^*\left(6I_3 - AA^*\right)^{-1}A\right)C^*,$$

which, by Lemma 2.7 and (19) is

$$C\left(I_3 + \frac{1}{6}A^*\left(I_3 - \frac{1}{6}AA^*\right)^{-1}A\right)C^* = C\left(I_3 - \frac{1}{6}A^*A\right)^{-1}C^* = 6C\left(C^*C\right)^{-1}C^* = 6I_3.$$

$\square$

We do not state that the obtained unitary matrix U is Hadamard, which is not true in general. Recall that our goal is to embed the submatrix E into the matrix G_6 (cf. (1)-(2)). We have the following trivial

Lemma 2.9. *Suppose that a submatrix E can be embedded into a complex Hadamard matrix G_6 of order 6 in which the upper right submatrix B is invertible. Then for some unimodular submatrix C for which the first three columns of G_6 are orthogonal the lower right submatrix $D = -CE^*(B^{-1})^*$ is unimodular.*

Proof. Indeed, this is exactly what embedding means. $\square$

In particular, if the submatrices B and C are chosen carefully, the unimodular property of D follows for free.

Corollary 2.10. *Start from a submatrix E and suppose that there are only finitely many (invertible) candidate matrices $B \in SOL_B$ and $C \in SOL_C$ such that the first three rows and columns of the matrix G_6 are orthogonal. Then E can be embedded into a complex Hadamard matrix of order 6 if and only if there is some $B \in SOL_B$ and $C \in SOL_C$ such that the matrix $D = -CE^*(B^{-1})^*$ is unimodular.*

Note that due to the finiteness condition in Corollary 2.10 once we have all (but finitely many) candidate matrices B and C we can decide algorithmically whether the submatrix E can be embedded into a complex Hadamard matrix.

The next step is to characterize 6×6 complex Hadamard matrices with vanishing 3×3 minors. To do this we need two auxiliary results first.

Lemma 2.11. *Suppose that in a dephased 6×6 complex Hadamard matrix there exist a noninitial row (or column) containing three identical entries x. Then $x = \pm 1$ and this row (or column) reads $(1, 1, 1, -1, -1, -1)$, up to permutations.*

Proof. Suppose to the contrary, that there are three nonreal numbers x in a row (column). Then the sum of these numbers x together with the leading 1 read $|1+3x|^2 = 10+6\Re(x) > 4$, and hence, by Lemma 2.1 this row (column) cannot be orthogonal to the first row (column), a contradiction. To ensure orthogonality to the first row (column) we should specify the remaining three entries to $-x$ and hence the last part of the statement follows.   □

Recall that the core of a dephased complex Hadamard matrix of order n is its lower right $(n-1) \times (n-1)$ submatrix. A vanishing sum of order k is a k-term sum adding up to 0. The following breakthrough result was obtained very recently.

Theorem 2.12 ((Karlsson, [9, 10])). *Let H be a dephased complex Hadamard matrix of order 6. Then the following are equivalent:*

(a) H belongs to the three-parameter degenerate family $K_6^{(3)}$;
(b) H is H_2-reducible;
(c) The core of H contains a -1;
(d) Some row or column of H contains a vanishing sum of order 2;
(e) Some row or column of H contains a vanishing sum of order 4.

In particular, Theorem 2.12 gives a characterization of complex Hadamard matrices of order 6 containing F_2 as a submatrix. The term H_2-reducibility refers to the beautiful structure of these matrices: they have a canonical form in which all 9 of their 2×2 submatrices are complex Hadamard. Part (c) and (d) of Theorem 2.12 allow us to quickly recognize if a matrix belongs to the family $K_6^{(3)}$, and we shall heavily use these conditions through our paper. Part (e) tells us that once we have four entries in a row or column of a matrix which lies outside the family $K_6^{(3)}$ the Decomposition formula readily derives the unique remaining two values through (4). As the family $K_6^{(3)}$ forms a three-parameter subset, the matrices it contains are atypical, hence the adjective "degenerate".

Corollary 2.13. *Suppose that in a dephased 6×6 complex Hadamard matrix H there exist a noninitial row (or column) containing three identical entries. Then H belongs to the family $K_6^{(3)}$.*

Lemma 2.14. *Suppose that a 6×6 complex Hadamard matrix H has a vanishing 3×3 minor. Then H belongs to the family $K_6^{(3)}$.*

Proof. Suppose that H has a vanishing 3×3 minor, say the upper left submatrix $E(a, b, c, d)$, as in formula (1). Such an assumption can be made, up to equivalence. As $\det(E) = b + c - a - d + ad - bc = 0$, we find that if any of the indeterminates a, b, c, d is equal to 1 then E contains a noninitial row (or column) containing three 1s, and therefore by Corollary 2.13 we conclude that this matrix belongs to the family $K_6^{(3)}$. Otherwise, we can suppose that none of a, b, c, d is equal to 1 and hence we find that $d = (a + bc - b - c)/(a - 1)$, which should be of modulus one. To ensure this solve the equation $d\bar{d} - 1 = 0$ to find that either $b = a$ or $c = a$ should hold, but then we have either $d = c$ or $d = b$ as well. In particular, we find that E has two identical rows (or columns). After enphasing the matrix, again, we find that there is a full column (or row) of entries 1 and a reference to Corollary 2.13 concludes the lemma. $\square$

Therefore to investigate those matrices which lie outside the family $K_6^{(3)}$ we can safely use Lemma 2.8 and in particular the inversion formula (20).

It turns out, that the isolated matrix $S_6^{(0)}$ (cf. [18]) requires a special treatment as well. It is featured in the following

Lemma 2.15. *Suppose that in a 6×6 dephased complex Hadamard matrix H there is a noninitial row and column composed of cubic roots of unity. Then H is either equivalent to $S_6^{(0)}$ or belongs to the family $K_6^{(3)}$.*

Let us denote by ω the principal cubic root of unity once and for all, that is $\omega := \mathbf{e}^{2\pi \mathbf{i}/3}$.

Proof. First suppose that the cubic row and column meet in a common 1. Then our matrix looks like as the matrix H on the left below, up to equivalence:

$$
H = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\
1 & \omega & a & b & c & d \\
1 & \omega & * & * & * & * \\
1 & \omega^2 & * & * & * & * \\
1 & \omega^2 & * & * & * & *
\end{bmatrix}, \quad
H' = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\
1 & a & 1 & b & c & d \\
1 & * & \omega & * & * & * \\
1 & * & \omega^2 & * & * & * \\
1 & * & \omega^2 & * & * & *
\end{bmatrix}.
$$

Now by orthogonality of the first three rows we find that $a + b = -\omega$ and $c + d = -1$. Hence, we can assume, up to equivalence, that $a = 1, b = -\omega^2$, and $c = \omega$, $d = \omega^2$. But then, we can fill out the fourth row, and the third and fourth column as well. We conclude that the obtained matrix is equivalent to $S_6^{(0)}$.

Secondly, let us suppose that the cubic row and column meet in a common ω. This matrix H' is depicted on the right above. Then, by calculating the orthogonality equations, we find that either $a = -1$, and hence the matrix (if it can be completed to a Hadamard at all) belongs to the family $K_6^{(3)}$, or $a = \omega$, $b = \omega^2$, and, up to equivalence $c = \omega$, $d = \omega^2$. This implies that the third row and third column feature cubic entries only meeting in a common 1 therefore reducing the situation to the first case. The third case, namely when the cubic row and column meet in a common ω^2 can be treated similarly. $\square$

Now we turn to the presetting of the submatrix $E(a, b, c, d)$ (see (1)). In order to avoid the case when the system of equations (5)–(17) is linearly dependent we need to exclude various input quadruples (a, b, c, d). However, it shall turn out that we are free to do such

restrictions, up to equivalence. Before proceeding further, let us define the following two-variable function mapping $\mathbb{T}^2$ to $\mathbb{C}$ as follows:

$$\mathcal{E}(x,y) := x + y + x^2 + y^2 + xy^2 + x^2 y.$$

We say that y is an elliptical pair of x, if $\mathcal{E}(x,y) = 0$. Observe that for a given $x \neq -1$ the sum of its elliptical pairs read $y_1 + y_2 = -(1 + x^2)/(1 + x)$. The following is a strictly technical

Proposition 2.16 ((Canonical transformation)). *Suppose that we have a complex Hadamard matrix H inequivalent from $S_6^{(0)}$ and any of the members of the family $K_6^{(3)}$. Then H has a 3×3 submatrix $E(a,b,c,d)$ as in formula* (1), *up to equivalence, satisfying*

(21) $$(b-1)(c-1)(b-d^2)(c-d^2)(b-c)(bc-d)\mathcal{E}(b,d)\mathcal{E}(c,d) \neq 0.$$

Proof. The strategy of the proof is the following: first we pick a "central element" d from the core of the matrix and then we show that b and c can be set satisfying (21). Recall, that by Lemma 2.15 there is no a noninitial row and column composed from cubic roots of unity in the matrix.

First let us assume that there is a 1 in the core somewhere. Suppose that there is a, to say, row full of cubics. In this case set $d = \omega$, and $c = \omega^2$. Now in the column containing d there is a non-cubic entry γ, and we are free to set $b = \gamma$. If there is neither a full row nor a column of cubics in the matrix, then set $d = 1$, and choose a non-cubic c from its row. Note that there cannot be a further noninitial 1 in the row or column of d by Corollary 2.13. Now observe that as the elliptical pairs of 1 are ω and ω^2, we can choose a suitable b from the column of d unless all entries there are members of the set $\{\omega, \omega^2, c, \overline{c}\}$. Note that ω together with ω^2 cannot be in the column of d at the same time, and from this it is easily seen that we cannot define the value of b only if the column of d is one of the following four cases, up to permutations: $(1, 1, \omega, c, c, \overline{c})$, $(1, 1, \omega, c, \overline{c}, \overline{c})$, $(1, 1, \omega^2, c, c, \overline{c})$, $(1, 1, \omega^2, c, \overline{c}, \overline{c})$. However, by normalization and by orthogonality, the sum of the entries in this column should add up to 0, and we find in all cases that the unimodular solution to c is a cubic root of unity, contradicting the choice of c. Therefore one of the entries in the column of d is different from $\omega, \omega^2, c, \overline{c}$ which will be chosen as b.

Secondly, let us suppose, that there is no 1 in the core. In particular, all entries in the core are different rowwise and columnwise.

Pick any d from the core of the matrix. Let us denote by c_1 and c_2 the elliptical pairs of d (maybe $c_1 = c_2$, or they are undefined). Now we have several cases depending on the appearance of these values in the row and column containing d.

CASE 1: c_1 and c_2 present in both the row and column containing d. Hence, in the row and column containing d there are the entries 1, d, c_1 and c_2 already, the remaining two, α and β are uniquely determined by the Decomposition formula. Note that $\alpha \neq d^2$, as otherwise we would have $\beta = -(2d + d^2 + d^3)/(1 + d)$ (as the sum of all entries in a noninitial row add up to 0, and the sum of the elliptical pairs is known), which is unimodular if and only if $d = \pm\mathbf{i}$ or $d = \omega$ or $d = \omega^2$. In the first case we have $\beta = \mp\mathbf{i}$ and we are dealing with a member of the family $K_6^{(3)}$. The second and third case imply that we have a full row and a full column of cubics, a contradiction. If $\beta \neq d/\alpha$ then by picking $c = \alpha$ from the row we can set $b = \beta$ in the column. Otherwise, in case we have $\beta = d/\alpha$, then reset the central element d to the α which is in the same row as d. Now observe that after this exchange we should met the requirements of Case 1 again (otherwise we are done here), and hence the elliptical

pairs of α, α_1 and α_2, should present in the row and column of α, which therefore contain exactly the same entries. However $\alpha_{1,2} \neq d$, as otherwise orthogonality with the condition $\mathcal{E}(\alpha, d) = 0$ would imply $d = \pm 1$, a contradiction; $\alpha_{1,2} \neq d/\alpha$, as otherwise $d = \omega$ or $d = \omega^2$ would follow from the same argument implying that the row containing α has a noninitial 1, a contradiction. Therefore, the only option left is that $\alpha_{1,2} = c_{1,2}$. But then we can set $c = d \neq \alpha^2$ and $b = d/\alpha \neq \alpha^2$, and we are done.

CASE 2: c_1 and c_2 present in (to say) the row containing d, but only one of these values (say c_1) is present in the column of d. Let us denote by α and β the two further entries in this row which, again, are different from d^2. In the column of d there is already 1, d and c_1, and observe that the remaining three entries cannot be (d^2, α, β) as this would imply $d^2 = c_2$, contradicting our case-assumption. Therefore one of the three unspecified entries γ is different from d^2, α and β. Now if $\gamma \neq d/\alpha$ then set $c = \alpha$, $b = \gamma$ otherwise set $c = \beta$, $b = \gamma$. We are done.

CASE 3: Only the value c_1 is in (to say) the row containing d and in the column of d as well. This is a tricky case, as it might happen that the undetermined triplet in both the d-th row and column is precisely $(d^2, \alpha, d/\alpha)$, and therefore we cannot ensure condition (21). However, from the orthogonality equation $1 + d + d^2 + c_1 + \alpha + d/\alpha = 0$, from its conjugate, and the elliptical condition $\mathcal{E}(c_1, d) = 0$ we can form a system of equations, the solution of which can be found by computing a Gröbner basis. By investigating the results, we find that either $\alpha = -1$ or $\alpha + d = 0$ leading us to the family $K_6^{(3)}$ or $c_1 = \overline{d}$. In the last case, however, we can calculate the values of d and α explicitly. In particular, we find that the values of d and α are given by some of the unimodular roots of the following polynomials $1 + 2d + 2d^3 + d^4 = 0$ and $1 + 4\alpha - 2\alpha^2 - 8\alpha^3 - 8\alpha^4 - 8\alpha^5 - 2\alpha^6 + 4\alpha^7 + \alpha^8 = 0$. Now reset the "central" entry d to α, and observe that the elliptical pairs of α are not present in its row, and therefore the conditions of this subcase are no longer met. Otherwise we can suppose that the undetermined triplet in the column of d is not $(d^2, \alpha, d/\alpha)$. Set $c = \alpha \neq d^2$. Pick γ from the column which is different from d^2, α, d/α, set $b = \gamma$ and we are done.

CASE 4: Only the value c_1 is in (to say) the row containing d and in the column of d there is the other elliptical value $c_2 \neq c_1$. We can suppose that two of the undetermined entries in the row of d satisfy $\alpha \neq d^2$ and $\beta \neq d^2$ and set $c = \alpha$. Now if in the column the undefined triplet is precisely $(\alpha, d/\alpha, d^2)$, then observe that the same triplet cannot appear in the row, as otherwise $c_1 = c_2$ would follow. Therefore we can reset c to a value different from $\alpha, d/\alpha, d^2$, and set $b = \alpha$. Otherwise there is an entry in the column which can be set to b, we are done.

CASE 5: In the column of d there is no elliptical value at all. Pick any $c = \alpha \neq d^2$ from the row. Now in the column there are four unspecified entries. Clearly, one of them, say γ will be different from d^2, α and d/α. Set $b = \gamma$. We are done. $\qquad\square$

Not every submatrix E can be embedded into a complex Hadamard matrix of order 6. To offer a necessary condition, let us recall first that an operator A is called a contraction, if $\|A\|_2 \leq 1$, where $\|.\|_2$ denotes both the Euclidean norm on $\mathbb{C}^6$ and the induced operator norm on the space of 6×6 matrices. We have the following

Lemma 2.17. *If A is any 3×3 submatrix of a complex Hadamard matrix H of order 6 then $A/\sqrt{6}$ is a contraction.*

Proof. Clearly, we can assume that this submatrix A is the upper left of the matrix H, which we will write in block form, as follows:

$$H = \begin{bmatrix} A & B \\ C & D \end{bmatrix}.$$

Now suppose, to the contrary that there is some vector s, such that $\|As\|_2 > \sqrt{6} \|s\|_2$ and consider the block vector $s' := (s, 0)^T \in \mathbb{C}^6$. We have

$$\|Hs'\|_2 = \left\|(As, Cs)^T\right\|_2 \geq \left\|(As, 0)^T\right\|_2 = \|As\|_2 > \sqrt{6} \|s\|_2 = \sqrt{6} \|s'\|_2 = \|Hs'\|_2,$$

where in the last step we used that the matrix $H/\sqrt{6}$ is unitary. $\square$

In particular, we have the following

Corollary 2.18. *If the submatrix E can be embedded into a complex Hadamard matrix of order 6, then every eigenvalue λ of the matrix E^*E satisfy $\lambda \leq 6$.*

Corollary 2.18 is a useful criterion to show that a matrix E cannot be embedded into a complex Hadamard matrix, however, it is unclear how to utilize it for our purposes. In particular, we do not know how to characterize those 3×3 matrices which satisfy its conditions. Also it is natural to ask whether the presence of the large eigenvalues is the only obstruction forbidding the submatrix E to be embedded. The answer to this question might depend on the dimension, as it is easily seen that while every 2×2 matrix can be embedded into a complex Hadamard matrix of order 4, only a handful of very special 2×2 matrices can be embedded into a complex Hadamard matrix of order 5 due to the finiteness result of Haagerup [7].

Now we are ready to present a new, previously unknown family of complex Hadamard matrices. The next section gives an overview of the results.

3. THE CONSTRUCTION: A HIGH-LEVEL PERSPECTIVE

Here we describe the generic family $G_6^{(4)}$ from a high-level perspective. In particular, we outline the main steps only, and do not discuss some degenerate cases which might come up during the construction. The next section is dedicated to investigate the process in details. The main result of this paper is the following

Construction 3.1 ((The Dilation Algorithm)). *Do the following step by step to obtain complex Hadamard matrices of order 6.*

#1: INPUT: the quadruple (a, b, c, d), forming the upper left 3×3 submatrix $E(a, b, c, d)$, as in formula (1).

#2: Use Haagerup's trick to the first three rows of $G_6^{(4)}$ (see (2)) to obtain a quadratic equation to f:

$$(22) \qquad\qquad \mathcal{F}_1 + \mathcal{F}_2 f + \mathcal{F}_3 f^2 = 0,$$

where the coefficients $\mathcal{F}_1$, $\mathcal{F}_2$ and $\mathcal{F}_3$ depend on the parameters a, b, c, d and the indeterminate e, and derive the following linearization formula from it:

$$(23) \qquad\qquad f^2 = -\frac{\mathcal{F}_1}{\mathcal{F}_3} - \frac{\mathcal{F}_2}{\mathcal{F}_3} f.$$

#3: Use Theorem 2.4 to obtain another quadratic equation to f:

$$\mathcal{G}_1 + \mathcal{G}_2 f + \mathcal{G}_3 f^2 = 0, \tag{24}$$

where, again, the coefficients $\mathcal{G}_1$, $\mathcal{G}_2$ and $\mathcal{G}_3$ depend on the parameters a, b, c, d and the indeterminate e. Plug the linearization formula (23) into (24) and rearrange to obtain the companion value of e $f = F(e)$, where

$$F(e) := -\frac{\mathcal{F}_3 \mathcal{G}_1 - \mathcal{F}_1 \mathcal{G}_3}{\mathcal{F}_3 \mathcal{G}_2 - \mathcal{F}_2 \mathcal{G}_3}. \tag{25}$$

#4: As $|f| = 1$ should hold, calculate the sextic polynomial $G(e)$ coming from the equation $F(e)\overline{F(e)} - 1 = 0$ and solve it for e.

#5: Amongst the roots of G find all unimodular triplets (e, s_1, s_2) satisfying $e + s_1 + s_2 = -1 - a - b$, calculate the companion values $f = F(e)$, $s_3 = F(s_1)$ and $s_4 = F(s_2)$ through formula (25) and store all sextuples $(e, s_1, s_2, f, s_3, s_4)$ in a solution set called SOL_B.

#6: Repeat steps #2–#6 to the transposed matrix (i. e. to the first three columns), mutatis mutandis to obtain the solution set SOL_C.

#7: For every pair of sextuples from SOL_B and SOL_C construct the submatrices B and C, check if the first three rows and columns are mutually orthogonal and finally use Lemma 2.8 to compute the lower right submatrix D through formula (20).

#8: OUTPUT: all unimodular matrices found in step #7.

Construction 3.1 gives the essence of the new family discovered, and in the next section we shall give it a mathematically rigorous, low-level look.

4. The construction: The nasty details

Here we investigate the steps of Construction 3.1 in details.

STEP #1: Choose a quadruple (a, b, c, d) in compliance with the Canonical Transformation described by Proposition 2.16 as the INPUT, and form the submatrix E. Check if it meets the requirements of Corollary 2.18; if yes, then proceed, otherwise conclude that it cannot be embedded into a complex Hadamard matrix of order 6. Experimental results show that once three out of the four parameters are fixed the last one can be easily set to a value such that the quadruple (a, b, c, d) leads to a complex Hadamard matrix. Heuristically this means that there is nothing "mystical" in the choice of the initial quadruple and hence the parameters should be independent from each other.

STEP #2: To obtain formula (23) we need to see that $\mathcal{F}_3 \not\equiv 0$, independently of e. Indeed, suppose otherwise, which means that the following system of equations (where the last two are the conjugate of the first two, up to some irrelevant constant factors)

$$\begin{cases} abc + a^2bc + abd + ab^2d + a^2bcd + ab^2cd & \equiv\ 0, \\ b^2c + ab^2c + a^2d + a^2bd + acd + bcd & \equiv\ 0, \\ a + b + ac + abc + bd + abd & \equiv\ 0, \\ a^2b + ab^2 + bc + b^2c + ad + a^2d & \equiv\ 0, \end{cases}$$

are fulfilled. We compute a Gröbner basis and find that the polynomial

$$bc(1 + c^2)(c - d)d(1 + d^2)(c^2 + d^2)(1 + d + d^2)$$

is a member of it. After substituting back into the original equations we find that there is either a vanishing sum of order 2 in E or $a = b = 1$ and therefore the whole family is a member of $K_6^{(3)}$, or we have $E = F_3$ or $E = F_3^*$ but these matrices have $b = c$ which however is not allowed by the Canonical Transformation.

It might happen that $\mathcal{F}_3 \not\equiv 0$ but there is a unimodular e making it vanish, which cannot be anything else, but

$$(26) \qquad e = \frac{a^2b + a^2d + ab^2 + ad + b^2c + bc}{abc + abd + ac + a + bd + b}.$$

Nevertheless, we can suppose that in case of one of the pairs (e, f), (s_1, s_3) and (s_2, s_4) we do not set e as above, otherwise we would have $e = s_1 = s_2$ which, by Lemma 2.11 would imply $e = s_1 = s_2 = -1$, obtaining some member of the family $K_6^{(3)}$ by Corollary 2.13. Hence, we can suppose that e is different than the value described by formula (26) above, and we conclude that $\mathcal{F}_3 \neq 0$.

STEP #3: Clearly, one cannot expect to recover a unique f from e in general, as formula (25) might suggests. Indeed, there are complex Hadamard matrices in which $s_1 = e$, but $s_3 \neq f$. The reason for this phenomenon is that formulas (22) and (24) might be linearly dependent. After plugging (23) into (24) we obtain the expression

$$\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3 + (\mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3)\, f = 0,$$

which can lead us to one of the following three cases:

CASE 1: Both the polynomials $\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3$ and $\mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3$ vanish identically, independently of e, meaning that in this case we do not have another condition on f. Luckily this can never happen, as by calculating a Gröbner basis (again, to speed up the computations we have added the conjugates of the equations as well) we find that the polynomial

$$(b-1)b^2(b-c)c(bc-d)(1+c+d)(b-d^2)\mathcal{E}(c,d)$$

is a member of the basis. Therefore we have either $c + d = -1$ or one of the degenerate cases described in the Canonical Transformation. The case $c + d = -1$ implies that the set $\{c, d\}$ consists of nontrivial cubic roots only. By directly solving the corresponding equations, we find that the quadruples $(1, 1, \omega, \omega^2)$, $(\omega^2, \omega, \omega, \omega^2)$ and $(1, 1, \omega^2, \omega)$, $(\omega, \omega^2, \omega^2, \omega)$ can vanish both polynomials, however these cases were excluded by the Canonical Transformation.

CASE 2: Both the polynomials $\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3$ and $\mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3$ vanish for some $|e| = 1$, meaning that in this case we do not have another condition on f. However, having these numbers e at our disposal we can recover the two possible values of f from (23). Once we have the candidate pairs (e, f_1) and (e, f_2) we readily calculate the remaining pairs (s_1, s_3) and (s_2, s_4) through the Decomposition Formula. Store all suitable sextics $(e, s_1, s_2, f, s_3, s_4)$ in the solution set SOL_B. Proceed to step #6.

CASE 3: One cannot set (or have not set in Case 2) a unimodular e to make these two polynomial vanish at the same time. Hence we can derive formula (25) for $F(e)$. Proceed to step #4.

STEP #4: Next we need to ensure that f is of modulus one. To do this, we calculate the fundamental polynomial

$$\mathcal{P}_{a,b,c,d}(e) \equiv |\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3|^2 - |\mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3|^2.$$

After some calculations, it will be apparent that $\mathcal{P}$ has the following remarkable structure:

$$\mathcal{P} \equiv a^8b^8c^6d^6\overline{P} + a^8b^8c^6d^6\overline{P}(2 + 2\overline{a} + 2\overline{b})e + a^8b^8c^6d^6\overline{Q}e^2 + Re^3 + Qe^4 + P(2 + 2a + 2b)e^5 + Pe^6$$

where the coefficients P, Q and R depend on the quadruple (a, b, c, d) only. If $\mathcal{P} \equiv 0$ then the construction fails. Otherwise we find all possible roots of $\mathcal{P}(e)$ of modulus one.

STEP #5: If the number on the right hand side of (26) is not of modulus one, then the rôle of the pairs $(e, f), (s_1, s_3)$ and (s_2, s_4) is symmetric, and from all of the roots of $\mathcal{P}$ of modulus one we select all possible triplets (e, s_1, s_2) satisfying $e + s_1 + s_2 = -1 - a - b$, which is needed to ensure orthogonality of the first two rows. From (25) we compute the unique companion values $f = F(e), s_3 = F(s_1)$ and $s_4 = F(s_2)$.

Otherwise, should the number on the right hand side of (26) is of modulus one, then for every root e of $\mathcal{P}$ we calculate its unique companion value $f = F(e)$, and then we use the Decomposition formula to determine the pairs (s_1, s_3) and (s_2, s_4).

If no unimodular roots are found at this point then the matrix $E(a, b, c, d)$ cannot be embedded into a complex Hadamard matrix of order 6, and we do not proceed any further.

At the end of this step we store all obtained sextics $(e, s_1, s_2, f, s_3, s_4)$ in the solution set SOL_B. Typically two sextics are found.

STEP #6: In this step one constructs the first three columns along the lines of steps #2–#5 described above and obtain the set SOL_C in a similar way.

STEP #7: For every candidate solution from SOL_B and SOL_C we check if the first three rows and columns are orthogonal, disregard those cases in which the submatrix B is singular and finally use Lemma 2.8 to obtain the lower right submatrix D. Note that by Lemma 2.14 we disregard members of the family $K_6^{(3)}$ only. We check if D is composed of unimodular entries.

STEP #8: Finally, we OUTPUT all unimodular matrices found during the process. We remark here that by Corollary 2.10 if no unimodular matrices were found then the submatrix E cannot be embedded into any complex Hadamard matrices of order 6. If unimodular matrices are found, then typically we find two matrices, as the solution set SOL_B and SOL_C contains two suitable sextics each, however, experimental results show that for each sextic in SOL_B there is a unique sextic in SOL_C making D unimodular as required.

We have finished the discussion of Construction 3.1. The results are summarized in the following

Theorem 4.1. *Start from a submatrix E as in* (1) *and suppose that there are only finitely many (invertible) candidate submatrices B and C such that the first three rows and columns of the matrix G_6 (see* (2)*) are orthogonal. Then Construction 3.1 gives an exhaustive list of all complex Hadamard matrices of order 6, up to equivalence, containing E as a submatrix.*

The interested reader might want to see an example of generic Hadamard matrices which can be described by closed analytic formulæ, that is for which the fundamental polynomials $\mathcal{P}_{a,b,c,d}$ and $\mathcal{P}_{a,c,b,d}$ are both solvable. Such a matrix can be obtained when we choose the input quadruple $(a, \overline{a}, c, a)$ where the real part of a is the unique real solution of $4\Re[a]^3 - 2\Re[a] + 1 = 0$ and $c = (-a^3 + a^2 + a + 1)/(a^4 + a^3 + a^2 - a)$. It is easily seen that the matrices we obtain starting from the submatrix $E(a, \overline{a}, c, a)$ are inequivalent from $S_6^{(0)}$ and do not belong to the family $K_6^{(3)}$.

Remark 4.2. When $\mathcal{P} \equiv 0$ then the main difficulty we are facing with is that we have infinitely many candidate submatrices B. In this case we have the trivial restriction (3) on e, while the companion value f coming from (25) is unimodular unconditionally. Although

in principle we can find three orthogonal rows through the Decomposition formula for every suitable e, we do not know which one to favourize in order to obtain a unimodular submatrix D via formula (20). Also, it might happen that the polynomial $\mathcal{P}_{a,c,b,d}$ obtained during step #6 shall vanish as well bringing another free parameter into the game making things even more complicated. In contrast, if both $\mathcal{P}_{a,b,c,d} \not\equiv 0$ and $\mathcal{P}_{a,c,b,d} \not\equiv 0$, then we have a finitely many choices for the submatrices B and C and we can use Corollary 2.10 to conclude the construction.

Remark 4.3. The polynomial $\mathcal{P}$ formally can vanish when we have $\mathcal{F}_3\mathcal{G}_1 - \mathcal{F}_1\mathcal{G}_3 \equiv \mathcal{F}_3\mathcal{G}_2 - \mathcal{F}_2\mathcal{G}_3 \equiv 0$, however this is excluded by the Canonical Transformation and explained in details in Case 1 of step #3. It might vanish for some other, non-trivial quadruples as well making the whole construction process fail. In theory, the common roots of the coefficients of $\mathcal{P}$ can be calculated by means of Gröbner bases, but as these coefficients are rather complicated obtaining such a basis turned out to be a task beyond our capabilities. Nevertheless, we conjecture that the case $\mathcal{P} \equiv 0$ can be excluded completely in a similar fashion as we disregarded various quadruples during the Canonical Transformation. This would mean that all complex Hadamard matrices of order 6, except from $S_6^{(0)}$ and $K_6^{(3)}$, can be recovered from Construction 3.1.

It is reasonable to think that every complex Hadamard matrix of order 6 has some 3×3 submatrix E leading to nonvanishing fundamental polynomials. In particular, we do not expect any complex Hadamard matrices of order 6 (except maybe $S_6^{(0)}$ and $K_6^{(3)}$) which cannot be recovered from Construction 3.1. Therefore we formulate the following

Conjecture 4.4. *The list of complex Hadamard matrices of order* 6 *is as follows: the isolated matrix* $S_6^{(0)}$*, the three-parameter degenerate family* $K_6^{(3)}$ *and the four-parameter generic family* $G_6^{(4)}$ *as described above.*

It would be nice to understand the structure of $G_6^{(4)}$ more thoroughly and express the entries of these matrices by some well-chosen trigonometric functions in a similar fashion as $K_6^{(3)}$ is described, however, as we have encountered sextic polynomials already the appearance of such formulas is somewhat unexpected. Also, it is natural to ask which matrices satisfy the conditions of Corollary 2.18. An algebraic characterization of these matrices might lead to a deeper understanding of the generic family $G_6^{(4)}$ and hopefully to the desired full classification of complex Hadamard matrices of order 6.

References

[1] K. Beauchamp and R. Nicoara, *Orthogonal maximal abelian $*$-subalgebras of the 6×6 matrices*, Linear Algebra and its Applications, **428**:8–9 (2008), 1833–1853.

[2] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej and K. Życzkowski, *Mutually unbiased bases and Hadamard matrices of order six*, J. Math. Phys. **48**, 052106 (2007)

[3] B. Buchberger, *An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal.*, PhD Thesis, Mathematical Institute, University of Innsbruck, Austria, 1965.

[4] R. Craigen, *Equivalence classes of inverse orthogonal and unit Hadamard matrices*, Bull. Austral. Math. Soc., **44** (1991), 109–115.

[5] P. Diţă, *Some results on the parametrization of complex Hadamard matrices*, J. Phys. A, **20** (2004), 5355–5374.

[6] C. Godsil and A. Roy, *Equiangular lines, mutually unbiased bases, and spin models*, European Journal of Combinatorics **30** (2009), 246–262.

[7] U. Haagerup, *Orthogonal maximal Abelian ∗-subalgebras of $n \times n$ matrices and cyclic n-roots*, Operator Algebras and Quantum Field Theory (Rome), MA International Press, (1996), 296–322.

[8] Ph. Jaming, M. Matolcsi, P.Móra, F. Szöllősi and M.Weiner, *A generalized Pauli problem and an infinite family of MUB-triplets in dimension* 6 , J. Phys. A: Math. Theor. **42** 245305

[9] B. R. Karlsson, *H_2-reducible Hadamard matrices of order* 6, Preprint, arXiv:1003.4133v1 [math-ph] (2010)

[10] B. R. Karlsson, *Three-parameter complex Hadamard matrices of order* 6, Preprint, arXiv:1003.4177v1 [math-ph] (2010)

[11] B. R. Karlsson, *Two-parameter complex Hadamard matrices for $N = 6$*, J. Math. Phys. 50, 082104 (2009)

[12] L. Lovász, Unpublished, (1984).

[13] M. N. Kolountzakis and M. Matolcsi, *Complex Hadamard matrices and the spectral set conjecture*, Collectanea Mathematica, Vol. Extra (2006), 281–291.

[14] M. Matolcsi and F. Szöllősi, *Towards a classification of 6×6 complex Hadamard matrices*, Open Systems & Information Dynamics, **15**:2 (2008), 93–108.

[15] S. Popa, *Orthogonal pairs of ∗-subalgebras in finite von Neumann algebras*, J. Operator Theory, **9** (1983), 253–268.

[16] A. J. Skinner, V. A. Newell and R. Sanchez *Unbiased bases (Hadamards) for six-level systems: Four ways from Fourier* J. Math. Phys. **50**, 012107 (2009)

[17] F. Szöllősi, *A 2-parameter family of complex Hadamard matrices of order 6, induced by hypocycloids*, Proc. Amer. Math. Soc. **138**:3 (2010) 921–928.

[18] W. Tadej and K. Życzkowski, *A concise guide to complex Hadamard matrices*, Open Syst. Inf. Dyn., **13** (2006), 133–177.

[19] T. Tao, *Fuglede's conjecture is false in 5 and higher dimensions*, Math Res. Letters, **11** (2004), 251–258.

[20] R. F. Werner, *All teleportation and dense coding schemes*, J. Phys. A, **34** (2001), 7081–7094.

[21] G. Zauner, "Quantendesigns: Grundzäuge einer nichtkommutativen Designtheorie", (German) [Quantumdesigns: The foundations of a noncommutative design theory], Ph.D thesis, Universität Wien, (available at http://www.mat.univie.ac.at/∼neum/ms/zauner.pdf), 1999.

Ferenc Szöllősi: Department of Mathematics and its Applications, Central European University, H-1051, Nádor u. 9, Budapest, Hungary.

E-mail address: `szoferi@gmail.com`